

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW HAMPSHIRE

**IN THE MATTER OF THE SEARCH OF
THE PREMISES KNOWN AS 26
COLONEL DANIELS DR, BEDFORD,
NEW HAMPSHIRE, DESCRIBED
FULLY IN ATTACHMENT A,
INCLUDING OUTBUILDINGS,
GARAGES, AND VEHICLES LOCATED
THEREON, AND THE PERSONS OF
THOSE PRESENT**

Case No. 1:20-mj-_____

Filed Under Seal – Level II

**AFFIDAVIT IN SUPPORT OF
APPLICATION FOR SEARCH WARRANT**

I, Shawn Serra, a Special Agent with Homeland Security Investigations ("HSI"), being duly sworn, depose and state as follows:

1. I have been employed as an HSI Special Agent since June of 2005, and am currently assigned to the Manchester, New Hampshire, Resident Office. I graduated from the University of Massachusetts, Lowell, Massachusetts with a Bachelor of Science Degree in Criminal Justice. In 2003, I graduated from the University of Massachusetts, Lowell, Massachusetts with a Master of Arts Degree in Criminal Justice. I have also received training in the areas of child sexual exploitation including violations pertaining to possession, distribution, and production of child pornography by attending a twenty-three-week training program at the Federal Law Enforcement Training Center (FLETC) in Glynco, Georgia. As part of my duties, I have observed and reviewed examples of child pornography (as defined in 18 U.S.C. § 2256) in various forms of media, to include digital/computer media. During the course of this investigation, I have also conferred with other investigators who specialize in computer forensics and who have conducted numerous investigations which involved child sexual exploitation offenses.

2. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises located at 26 Colonel Daniels Drive Bedford, NH (hereafter "SUBJECT PREMISES"), further described in Attachment A, including one residential dwelling; vehicles found on the SUBJECT PREMISES; any computer, computer media, and electronic media located therein; and the person of John David Boyden II, for the things described in Attachment B—specifically, evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Section 2252(a)(4)(B), which relates to the illegal possession of child pornography, and Title 18 United States Code. Section 2252A(a)(2), which relates to the illegal distribution of child pornography.

3. During the course of this investigation I have conferred with other investigators who have conducted numerous investigations and executed numerous search and arrest warrants which involved child exploitation and/or child pornography offenses. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The facts set forth in this affidavit are based in part on my personal knowledge, information obtained during my participation in this investigation, information from others, including law enforcement officers, my review of documents and computer records related to this investigation, and information gained through my training and experience.

STATUTORY AUTHORITY

4. This investigation concerns alleged violations of 18 U.S.C. § 2252(a)(4)(B) and 18 U.S.C. § 2252A(a)(2), related to the possession and distribution of child pornography in the District of New Hampshire. 18 U.S.C. § 2252(a)(4)(B) makes it a crime for any person to knowingly possess one or more images depicting a minor under the age of 18 engaged in

sexually explicit conduct. 18 U.S.C. § 2252A(a)(2) makes it a crime for any person to knowingly receive or distribute any child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

DEFINITIONS

5. “Child pornography” includes any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct where (A) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (B) the visual depiction was a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (C) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. 18 U.S.C. § 2256(8).

6. “Child Erotica,” as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, legally obscene or that do not necessarily depict minors in sexually explicit conduct.

7. “Computer,” as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1) as “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.” These devices include but are not limited to any data-processing hardware (such as central processing units, memory typewriters, mobile “smart” telephones, tablets, and self-contained “laptop” or “notebook” computers).

8. “Computer Server” or “Server,” as used herein, is a computer that is attached to a dedicated network and serves many users. A web server, for example, is a computer which hosts the data associated with a website. That web server receives requests from a user and delivers information from the server to the user’s computer via the Internet. A domain name system (“DNS”) server, in essence, is a computer on the Internet that routes communications when a user types a domain name, such as www.cnn.com, into his or her web browser. Essentially, the domain name must be translated into an Internet Protocol (“IP”) address so the computer hosting the web site may be located, and the DNS server provides this function.

9. “Computer hardware,” as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

10. “Computer software,” as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

11. “Computer-related documentation,” as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

12. “Computer passwords, pass-phrases and data security devices,” as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password or pass-phrase (a string of alpha-numeric characters) usually operates as a sort of digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software or digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

13. The “Internet” is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

14. “Internet Service Providers” (“ISPs”), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial-up, broadband based access via digital subscriber line (“DSL”) or cable television, dedicated circuits, or satellite

based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name –a user name or screen name, an “e-mail address,” an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an Internet Service Provider (“ISP”) over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password.

15. “Internet Protocol address” or “IP address” refers to a unique number used by a computer to access the Internet. IP addresses can be “dynamic,” meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be “static,” if an ISP assigns a user’s computer a particular IP address which is used each time the computer accesses the Internet. IP addresses are also used by computer servers, including web servers, to communicate with other computers.

16. “URL” is an abbreviation for Uniform Resource Locator and is another name for a web address. URLs are made of letters, numbers, and other symbols in a standard form. People use them on computers by clicking a pre-prepared link or typing or copying and pasting one into a web browser to make the computer fetch and show some specific resource (usually a web page) from another computer (web server) on the Internet.

17. “Minor” means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

18. The terms “records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures,

photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (“DVDs”), Personal Digital Assistants (“PDAs”), Multi Media Cards (“MMCs”), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

19. “Sexually explicit conduct” means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).

20. “Visual depictions” include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

PROBABLE CAUSE

21. Kik is a free application that can be downloaded on an Android or iOS device permitting users to chat with other individuals one-on-one and in groups as well as share pictures and videos. Each user has the ability to create a screen name which can be changed at any time. It uses a smartphone’s data plan or Wi-Fi to allow the user to transmit and receive messages, photos, videos, sketches, mobile webpages, and other content over the internet after the user registers a username.

22. Starting in February 2019, HSI Manchester began receiving child exploitation referrals from the Homeland Security Investigations, Cyber Crimes Center (C3). The 16 leads covered

activity from December 2018 through September 2019. These referrals were generated by the Kik messaging application through the use of PhotoDNA and SafePhoto.

23. PhotoDNA is a technology developed by Microsoft that computes hash values of images, video and audio files to identify similar images. A hash value is a numeric value of a fixed length that uniquely identifies data. PhotoDNA works by computing a unique hash that represents an image. This hash is computed such that it is resistant to alterations in the image, including resizing and minor color alterations. It works by converting the image to black and white, resizing it, breaking it into a grid, and looking at intensity gradients or edges. PhotoDNA allows identification of child pornography images based on matching hash values with images that have already been reviewed and determined to contain child pornography. According to Kik, it runs PhotoDNA on all profile picture, background photos, and some uploaded content to Kik. Anytime PhotoDNA positively matches an image to a previously identified image of child pornography, the Kik account is banned and a police report is generated. According to Kik, from the time of implementation of PhotoDNA technology, a Kik employee has reviewed all images identified by PhotoDNA technology before reporting the image to law enforcement.

24. The second technology used by Kik is known as “SafePhoto.” Kik has developed an internal hash matching system (similar to PhotoDNA) with a database of approximately 1.7 million known child exploitation image hash values. This system runs a hash value check against all images sent within Kik. When a user sends an image with a hash value that matches a child exploitation hash value in the database, the account is banned and a police report is automatically generated. In the instances where SafePhoto identified the file by hash, these files were not viewed by Kik. For these images the HSI Cyber Crime Center (C3) conducted its own analysis by taking the hash value identified by Kik and running it against a database of hash values

maintained in the National Child Victim Identification System (NCVIS). If the hash value matched an image in the NCVIS, then C3 provided the image maintained by NCVIS to me to review. In those cases, I did not open the image provided by Kik but just the image with the matching hash value maintained by NCVIS. Based on my knowledge of how hash matching works, I believe that the image obtained by NCVIS would be the same as the image reported by Kik.

25. In February 2019, HSI Manchester received a lead from Kik with a suspected image of child pornography uploaded in December 2018. The lead identified username **adbcef32b**, email address adokfkrksk@gmail.com. The name on the Kik account was Jacob D. The account was created December 18, 2018 from IP address 24.62.208.151 using an iPhone. The user also listed the birthday as February 17, 1981. According to Comcast's records, the subscriber for the IP address at that time was Maureen Boyden, 26 Colonel Daniels Drive, Bedford, NH. One of the emails listed as an email user Id was j3boyden@comcast.net. Kik has subsequently deactivated this account.

26. On August 20, 2019, New Hampshire Internet Crimes Against Children (ICAC) Investigator Deputy Mathew Fleming along with Officer Eli Krause of the Bedford Police Department interviewed John David BOYDEN at Boyden Family Chiropractic in Bedford, NH. During the interview, BOYDEN denied any knowledge or use of Kik. BOYDEN further advised he would speak with his son about Kik and offered it may have been his daughter's boyfriend.

27. After this interview, HSI received Kik lead packages in August 2019, October 2019, and February 2020 for Kik activity that occurred in April 2019. HSI also received Kik lead packages in October 2019, December 2019 and January 2020 for activity that occurred in May 2019, June 2019, and August 2019, respectively.

Activity in April 2019

28. On or about August 30, 2019, HSI Manchester received Kik leads for usernames **anonadbc, jb3donut, jdawg902, jdawg910, jman9102** and **idkadbc** for activity occurring in April 2019. All of these accounts were created from the same IP address and all of the image uploads occurred from that IP address as well; IP address 24.62.208.151.¹ Comcast was served with a Department of Homeland Security (DHS) Summons for the subscriber information associated with that IP address. According to Comcast, from April 11, 2019 through April 27, 2019, that IP address was assigned to Maureen Boyden, 26 Colonel Daniels Drive, Bedford, NH. One of the emails listed as an email user Id was j3boyden@comcast.net.

*Kik username **jb3donut***

29. According to the Kik lead received in August 2019, this username has associated email address j3boyden@gmail.com. The name on the account was Johnny J B. The account was created on August 27, 2018 using an iPhone. Kik has deactivated the account. Through the use of a SafePhoto hash match, Kik identified an image with the SHA1 base 16 hash value D8D8F5B5556067187C9C2CE00636180C1EE2D0A0 uploaded on April 10, 2019, 00:04:25 UTC by the user as possible child sexual abuse material (CSAM). The image named D8D8F5B5556067187C9C2CE00636180C1EE2D0A0.jpeg which HSI received and reviewed from the NCVIS database depicts a naked minor female and a clothed minor female holding an adult male's penis.

30. On or about October 30, 2019, HSI Manchester received another Kik lead regarding username **jb3donut** for activity occurring in April. Through the use of PhotoDNA, Kik

¹ Except where specifically identified, the accounts discussed herein were created at this IP address and uploads discussed herein occurred from this IP address. There may, however, have been other logins to the accounts from other IP addresses.

identified an image of suspected CSAM uploaded on April 10, 2019 at 00:04:11 UTC from IP address 24.62.208.151. The image named Image-jb3donut_jvz-UPLOADIP-24.62.208.151- UPLOADTIME-2019-04-10-1554854651712.UTC.jpg which HSI received and reviewed from the NCVIS database depicts a naked female, approximately 12-14 years old, on her hands and knees. Her knees are spread exposing her genitals and anus which are the focus of the image.

*Kik username **anonadbc***

31. According to the August lead, this username had associated email address anonadbcaofkejskd@gmail.com. The name on the account was Nobody Really. The account was created March 17, 2019 using an iPhone. Kik has deactivated the account.

32. Through the use of a SafePhoto hash match, Kik identified an image with the SHA1 base 16 hash value A930DA0EAC1639BEA01F8408288842519C6AC19A uploaded on April 9, 2019, 23:51:44 UTC by the user as possible CSAM. The image named A930DA0EAC1639BEA01F8408288842519C6AC19A.jpg which HSI received and reviewed from the NCVIS database, depicts a female performing oral sex on an adult male. Because of the close up picture and the angle at which the photo was taken, it is difficult to determine the approximate age of the female.

*Kik username **idkadbc***

33. The August lead with this username identified associated email address ciekdkewals@fiekdkek.com. The name on the account was Lovin Life. The account was created April 11, 2019 using an iPhone. Kik has deactivated this account.

34. Through the use of a SafePhoto hash match, Kik identified an image with the SHA1 base 16 hash value EACF279B484632788ECC7E4B22EC461DFA011C22 uploaded on April 12, 2019, 22:08:31 UTC by the user as possible CSAM. The image named

EACF279B484632788ECC7E4B22EC461DFA011C22.jpg which HSI received and reviewed from the NCVIS database depicts a female, approximately 6-8 years old kissing the side of an adult male's penis.

35. On or about February 4, 2020, HSI Manchester received another Kik lead for username **idkadbc** for activity that occurred in September 2019. The name on the account is listed as Lovin Life and the email address for is ciekdkekwal@fiekdkek.com. The account was created on April 11, 2019 from IP address 24.62.208.151 using an iPhone.

36. Through the use of PhotoDNA, Kik identified an image upload from this account on April 12, 2019 at 21:56:45 UTC that was suspected CSAM. The image file titled Image-idkadbc_1no-UPLOADIP-24.62.208.151-UPLOADETIME-2019-04-12-1555106205787.UTC.jpg depicts an 8-10 year topless female sitting in a chair with her legs spread and high cut jeans shorts pulled into her genitals. I believe this image constitutes child erotica.

*Kik username **jdawg910***

37. The August lead for this username identified associated email address cieoskeiwi@ckekis.com. The name on the account was þý What s j Up Dawg. The account was created on April 13, 2019, 00:15:18 UTC with an iPad.

38. Through the use of PhotoDNA, Kik identified an image upload from this account on April 20, 2019 at 21:04:57 UTC that was suspected CSAM. The image file titled Image-jdawg910_au0-UPLOADIP-24.62.208.151-UPLOADETIME-2019-04-20-1555794297730.UTC.png depicts a female approximately 5-8 years old with an adult penis in her mouth.

39. On or about January 20, 2020, HSI Manchester received another Kik lead regarding **jdawg910**. Through the use of a PhotoDNA hash match, Kik identified an image uploaded April

20, 2019 at 20:39:38 UTC by the user as possible child sexual abuse material (CSAM). The image depicts two pubescent topless females in a large body of water and has a logo in the top right corner for LS-Magazine.com. I believe that this image constitutes child erotica.

*Kik username **jdawg902***

40. The August lead associated with this username identified associated email address sjiejdiejjwebr@fjejjd.com. The name on the account was Nonna Urbusiness. The account was created on April 22, 2019 at 01:34:38 UTC with an iPad. Kik has deactivated the account.

41. Through the use of PhotoDNA, Kik identified an image upload from this account on April 22, 2019 at 21:52:16 UTC that was suspected CSAM. The image file titled Image-jdawg902_9na-UPLOADIP-24.62.208.151-UPLOADTIME-2019-04-22-1555969936758.UTC.png depicts a naked prepubescent female lying on her back with her legs spread exposing her genitals. There is BD-COMPANY BD-TEAM label in the bottom right corner of the image.

*Kik username **jman9102***

42. The August lead associated with this account included email address ckwsks@qel.com. The name on the account was Hey Yo. The account was created on April 27, 2019 at 02:37:03 UTC using an iPhone. Kik has deactivated the account.

43. Although this account was created from the IP address at the SUBJECT PREMISES discussed above, on April 27, 2019, this account also had activity from IP address 76.119.203.74. A DHS Summons for the subscriber information to Comcast revealed the subscriber of this account as Judy Post, service address 25 Eastward Ave, Pocasset, MA and billing address 40 Springwood Way, Manchester, NH. A Facebook profile for John D Boyden II is friends with a Judy Post on the social media platform Facebook.

44. Through the use of a SafePhoto hash match, Kik identified an image with the SHA1 base 16 hash value F98B6BF929EAA32FAB117A585ACFCCB42E7CB3AB uploaded on April 27, 2019, 17:11:41 UTC by the user as possible CSAM. The image named F98B6BF929EAA32FAB117A585ACFCCB42E7CB3AB.jpg received by HSI and reviewed from the NCVIS database depicts a naked prepubescent female lying on her back with her legs spread exposing her genitals and anus.

Activity in May 2019

45. On or about October 30, 2019, HSI Manchester received Kik leads regarding usernames **jb3man902**, **jmandawg902121**, and **jb3man9021** for activity occurring in May 2019. All of these accounts were created from the same IP address and all of the image uploads occurred from that IP address as well; IP address 24.62.208.151. Although I don't have subscriber information for the IP address in May 2019, this is the same IP address that in April was subscribed at the SUBJECT PREMISES and the usernames appear to be variations of each other.

*Kik username **jmandawg902121**,*

46. The email address doskxkrbwj@lol.com was associated with this username. The name on the account was Johnny Heyyy There. The account was created on May 27, 2019 using an iPad.

47. Through the use of PhotoDNA, Kik identified an image upload from this account on May 28, 2019 at 20:14:31 UTC that was suspected CSAM. The image file titled Image-jmandawg902121_m5a-UPLOADIP-24.62.208.151-UPLOADTIME-2019-05-28-1559074471796.UTC.png depicts a naked female, approximately 10-12 years old, lying on her back with her legs spread being anally penetrated by an adult male penis.

Kik username jb3man902

48. The email address associated with this username was jmandksdkwk@gmail.com. The name on the account was Johnny J B Man. The account was created on April 27, 2019 using an iPhone.

49. Through the use of a SafePhoto hash match, Kik identified an image with the SHA1 base 16 hash value 4D1ACAD62C533219ED57316D1D5F6026099B73D6 uploaded on May 1, 2019 at 01:16:23 UTC by the user as possible CSAM. The image named 4D1ACAD62C533219ED57316D1D5F6026099B73D6.jpg obtained and reviewed by HSI from the NCVIS database depicts a female, approximately 5-8 years old, putting an adult penis in her mouth.

Kik username jb3man9021

50. The email address associated with this username was djdjsajdj@dkekw.com. The name on the account was Hi World. The account was created on May 1, 2019 using an iPhone. Through the use of a SafePhoto hash match, Kik identified an image with the SHA1 base 16 hash value 43FF333F2FF9D6A2627F5AB3044935F3D16F2398 uploaded May 1, 2019 at 02:16:10 UTC by the user as possible CSAM. The image named 43FF333F2FF9D6A2627F5AB3044935F3D16F2398.jpg obtained and reviewed from the NCVIS database depicts a naked pubescent female lying on her back with her arms and legs spread exposing her genitals.

Activity from June 2019

51. On or about December 2, 2019, HSI Manchester received a Kik lead regarding username **jmandawg9021212** for activity that occurred on June 5, 2019. The email address for the account was listed as kfejsje@cksmmsm.ca. The name on the account lists first name “J” “JO”

“Jonny” “A”, last name Z. The account was created May 28, 2019 from IP address 24.62.208.151 using an iPhone.

52. Through the use of PhotoDNA, Kik identified an image upload from this account on June 5, 2019 at 1:30:03 UTC that was suspected CSAM. The image file titled Image-jmandawg9021212_l2h-UPLOADIP-24.62.208.151-UPLOADTIME-2019-06-05-1559698203328.UTC.png depicts a very close picture of a female’s genitals being spread apart by an adult’s fingers.

53. DHS Summons to Comcast for the subscriber information for IP address 24.62.208.151 for June 5, 2019, 01:34:12 UTC was unsuccessful because by the time the summons was issued, Comcast no longer retained the information.

54. On January 22, 2020, HSI received another Kik lead for the username **jmandawg9021212** based on a PhotoDNA hash. On May 30, 2019, this account uploaded an image named “Image-jmandawg9021212_l2h-UPLOADIP-24.62.208.151-UPLOADTIME-2019-05-30-1559258149700.UTC” depicting a naked prepubescent female sitting on a glass table with her legs spread exposing her genitals. The focus of the image is the female’s genitals. Again, the IP address at the time was 24.62.208.151.

Activity in August 2019

55. On or about January 22, 2020, HSI Manchester received a Kik lead regarding username **jmandawg9** for activity occurring in August 2019. Again the image upload and the account creation occurred from the same IP address, 24.62.208.151.

56. According to the lead, the Kik username **jmandawg9** had associated email akxkrnqjqidj@com.com. The name on the account was Johnny D. The account was created 07/19/2019 from IP address 24.62.208.151 using an iPad. Kik has deactivated this account.

57. Through the use of a SafePhoto hash match, Kik identified an image with the SHA1 base 16 hash value 0E8AF9C8F34B779BC94143117B3158651EBBF219 uploaded on August 17, 2019 at 17:45:01 UTC by the user as possible CSAM. This image was uploaded from IP address 24.62.208.151. The image named 0E8AF9C8F34B779BC94143117B3158651EBBF219.jpg retrieved and reviewed from the NCVIS database depicts a naked prepubescent female lying on her back with her legs spread exposing her genitals that appear to have ejaculate on them. The focal point of the image is the female's genitals.

June 2020 SNAPCHAT Lead

58. On June 4, 2020, the C3 sent HSI Manchester Cybertip 72657298 from the National Center for Missing and Exploited Children (NCMEC). Snapchat reported possible child pornography being uploaded using their application on April 15, 2020, 23:50:17 UTC, from IP address 24.62.208.151, by user Johnnydonuts13, email address j3boyden@gmail.com. A DHS Summons to Comcast for the subscriber information revealed that IP address was assigned to Maureen Boyden, 26 Colonel Daniels Drive, Bedford, NH, from April 15, 2020 to June 6, 2020. This is consistent with the subscriber information from the Kik information. According to the Snapchat CyberTip, when the image was posted, it was publicly available on the internet. The image associated with the tip depicts a minor female, approximately 12-14 years old, lying on her stomach, propped on her elbows, performing oral sex on an adult male. The female is clearly a child based on her small facial features, bone structure and lack of development.

59. Through various database searches, I have identified the following individuals with a home address of the SUBJECT PREMISES

- a. John David Boyden II, date of birth November 04, 1966.
- b. Maureen Jude Boyden, date of birth March 30, 1967

c. A juvenile male ("J.B."), date of birth September 10, 2002.

60. I believe the Boydens also have two adult children that no longer reside at the residence.

The following four vehicles are registered to the SUBJECT PREMISES to either John or Maureen Boyden.

- a. A 2002 beige, Toyota Sienna with NH tag 7916C. This vehicle has been observed at the residence on August 10, 17, 20 and 21, 2020.
- b. A 1998 brown, Toyota Camry with NH tag 3900697. This vehicle has been observed at the residence on August 10, 17, 20 and 21, 2020.
- c. A 2006 Silver Toyota Camry, with NH tag 4559864. On August 21, 2020, your affiant observed the previous two vehicles in the driveway at 6:40 A.M. At approximately 6:54 A.M. the Silver Camry left the driveway of the SUBJECT PREMISES. The operator of the Camry was a white male. Your affiant drove by the SUBJECT RESIDENCE while following the silver Camry and observed a third vehicle through the windows of the garage door on the left side of the garage, but was unable to ascertain the make and model. A short time later, the silver Camry was observed in the parking log of 40 S. River Road, Bedford, NH. It should be noted that Boyden Family Chiropractic is located in Suite 34 of this development.
- d. A 2014 silver Subaru Outback with NH tag C4471. This vehicle has not been observed at the SUBJECT PREMISES, but based on the morning surveillance of August 21, 2020, where 4 vehicles were observed at the SUBJECT PREMISES, two in the driveway, one leaving, and one in the garage, this is likely the vehicle

in the garage. I only seek authority to search this vehicle if it is at the SUBJECT PREMISES the day of the search.

COMPUTER ELECTRONIC STORAGE AND FORENSIC ANALYSIS

61. As described above and in Attachment B, this application seeks permission to search and seize records that might be found on the SUBJECT PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure and search of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

62. I submit that if a computer or storage medium is found on the SUBJECT PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being

used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating systems or application operations, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the internet are sometimes automatically downloaded into a temporary internet directory or “cache.”

e. Your Affiant is also aware, through training and experience, that digital storage devices have become interconnected, making it easy for even casual users of technology to transfer or copy images from one device to another, or to maintain duplicate copies on more than one device or storage medium. In fact, many devices such as smartphones can be set to automatically back up their contents to alternate storage facilities, such as laptop or desktop computers, another phone, photo-sharing websites, and cloud storage providers.

f. Your Affiant is aware that the contents of smart phones can be synched with or backed up to other digital devices in a variety of ways. Smartphones can be connected through cables to other devices, such as laptop computers, for data transfer.

Smartphones can also connect to other devices and transfer photos or documents wirelessly through technology such as Bluetooth. Data can also be sent from the phone to an email account via the Internet, and subsequently downloaded from the Internet to a different device (such as a tablet, game system, or computer) for storage. In addition, many smartphones utilize “cloud” storage. Cellular telephones can be set to automatically back up their contents to user accounts hosted on servers of various cloud storage providers. Users can also opt to perform a back-up manually, on an as-needed basis. Your Affiant is aware that some smartphones also back up their contents automatically to devices such as laptop computers. Additionally, cellular telephones can exchange data between two differing cellular communications devices and other types of electronic and media storage devices via Bluetooth or Wi-Fi, regardless of the type of operating system or platform being utilized to operate each of the electronic devices. In addition, media cards which contain many forms of data can be interchanged between multiple types of electronic devices, including but not limited to, different cellular telephones.

63. As set forth above, probable cause exists to believe that an individual at the SUBJECT PREMISES has distributed, received, or possessed child pornography. Based upon my knowledge and experience in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know that there are certain characteristics common to individuals involved in such crimes:

Those who distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books,

slides and/or drawings or other visual media. Such individuals often times use these materials for their own sexual arousal and gratification.

b. Those who distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes often possess and maintain copies of child pornography material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. These individuals typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

c. Those who distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. They often maintain these collections for several years and keep them close by, usually at the individual's residence, to enable the collector to view the collection, which is valued highly.

d. Those who distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes also may correspond with and/or meet others to share information and materials; they rarely destroy correspondence from other child pornography distributors/collectors; they conceal such correspondence as they do their sexually explicit material; and they often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

64. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any computer in the SUBJECT PREMISES because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.
- b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, “chat,” instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the

foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

65. Based on my training and experience I know that much of the media referenced above, which may contain contraband, fruits and evidence of crime, is by its very nature portable. This includes as example but is not limited to extremely compact storage devices such as thumb drives, laptop computers, and smart phones. In my training and experience, I know it is not uncommon for individuals to keep such media in multiple locations within their premises, including in outbuildings and motor vehicles, and/or on their person.

66. Searching storage media for the evidence described in the attachment may require a range of data analysis techniques. In most cases, a thorough search for information stored in storage media often requires agents to seize most or all electronic storage media and later review the media consistent with the warrant. In lieu of seizure, it is sometimes possible to make an image

copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. **The nature of evidence.** As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly search storage media to obtain evidence, including evidence that is not neatly organized into files or documents. Just as a search of a premises for physical objects requires searching the entire premises for those objects that are described by a warrant, a search of this premises for the things described in this warrant will likely require a search among the data stored in storage media for the things (including electronic data) called for by this warrant. Additionally, it is possible that files have been deleted or edited, but that remnants of older versions are in unallocated space or slack space. This, too, makes it exceedingly likely that in this case it will be necessary to use more thorough techniques.

b. **The volume of evidence.** Storage media can store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to peruse all the stored data to determine which particular

files is evidence or instrumentalities of a crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical and invasive to attempt this kind of data search on-site.

c. **Technical requirements.** Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on-site. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

d. **Variety of forms of electronic media.** Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

67. Based on the foregoing, and consistent with Rule 41(e)(2)(B), when officers executing the warrant conclude that it would be impractical to review the hardware, media, or peripherals on-site, the warrant I am applying for would permit officers either to seize or to image-copy those items that reasonably appear to contain some or all of the evidence described in the warrant, and then later review the seized items or image copies consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

BIOMETRIC ACCESS TO DEVICES

68. This warrant seeks authorization for law enforcement to compel all individuals present at the SUBJECT PRESMISES to unlock any DEVICES requiring biometric access subject to seizure pursuant to this warrant. Grounds for this request follow.

69. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

70. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called “Touch ID,” which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device’s Touch ID sensor, which is found in the round button (often referred to as the “home” button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

71. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called “Trusted Face”. During the Trusted Face registration process, the user holds the device in front of his or her face. The device’s front-facing camera then analyzes,

and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face.

Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

72. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

73. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents.

74. As discussed in this Affidavit, I have reason to believe that one or more digital devices will be found during the search. The passcode or password that would unlock the DEVICES subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the DEVICES, making the use of biometric features necessary to the execution of the search authorized by this warrant.

75. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

76. In light of the foregoing, and with respect to (1) any device found on the person of John Boyden II, or (2) any device at/on SUBJECT PREMISES reasonably believed to be owned, used, or accessed by John Boyden II, law enforcement personnel seek authorization, during execution of this search warrant, to: (1) press or swipe the fingers (including thumbs) of John Boyden II to the fingerprint scanner of the seized device(s); (2) hold the seized device(s) in front of the face of John Boyden II and activate the facial recognition feature; and/or (3) hold the seized device(s) in front of the face of that John Boyden II and activate the iris recognition feature, for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this warrant.

77. The proposed warrant does not authorize law enforcement to compel that an individual present at the SUBJECT PRESMISES state or otherwise provide the password or any other

means that may be used to unlock or access the DEVICES. Moreover, the proposed warrant does not authorize law enforcement to compel an individual present at the SUBJECT PRESMISES to identify the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the DEVICES.

CONCLUSION

78. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that evidence, fruits, and instrumentalities of the crime of possessing child pornography in violation of 18 U.S.C. § 2252(a)(4)(B) may be located at the SUBJECT PREMISES. I therefore seek a warrant to search the SUBJECT PREMISES described in Attachment A and any computer and electronic media located therein, and to seize the items described in Attachment B.

79. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the “return” inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

Dated: August 25, 2020

Respectfully Submitted,

/s/ Shawn Serra
Shawn Serra
Special Agent
Homeland Security Investigations

The affiant appeared before me by telephonic conference on this date pursuant to Fed. R. Crim. P. 4.1 and affirmed under oath the content of this affidavit and application.

Andrea K. Johnstone

Hon. Andrea K. Johnstone
United States Magistrate Judge
Dated: August 25, 2020

ATTACHMENT A
PREMISES TO BE SEARCHED

The premises to be searched includes:

The residential property located at This is single family, two story residence with an attached garage. The residence is a gray/blue color and has white shudders. The house is marked 26 to the right of the front door and the mailbox is marked 26.

1. The residential property located at 26 Colonel Daniels Dr., Bedford, NH, including any locked safes, storages containers, associated outbuildings and garages. This a single family two-story residence with an attached garage. It is a gray/blue color with white shutters. The house is marked 26 both to the right of the front door and on the mailbox.
2. Vehicles registered to the SUBJECT PREMISES and found at the SUBJECT PREMISES at the time of the search, to include:
 - i. A 2002 beige, Toyota Sienna with NH tag 7916C.
 - ii. A 1998 brown, Toyota Camry with NH tag 3900697.
 - iii. A 2006 Silver Toyota Camry, with NH tag 4559864.
 - iv. A 2014 silver Subaru Outback with NH tag C4471.
3. The person of John Boyden II, ()
4. The person of Maureen Jude Boyden, ()
5. A juvenile male (“J.B.”), ()

The following photograph depicts the SUBJECT PREMISES:



ATTACHMENT B
ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Sections 2252(a)(4)(B) and 2252A(a)(2):

1. All records relating to violations of 18 U.S.C. §§ 2252(a)(4)(B), 2252A(a)(2) in any form wherever they may be stored or found at the SUBJECT PREMISES, including:

- a. records and visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256;
- b. records or information pertaining to an interest in child pornography;
- c. records or information pertaining to the possession, receipt, transportation, or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;
- d. records or information of and relating to visual depictions that have been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct as defined in 18 U.S.C. § 2256, including the record or information used to create the visual depiction;
- e. records or information pertaining to Kik or Snapchat;
- f. photo-editing software and records or information relating to photo-editing software;

g. records or information relating to the occupancy or ownership of the SUBJECT PREMISES, including, but not limited to, utility and telephone bills, mail envelopes, vehicle registrations, tax bills, and other correspondence.

2. Any computer or electronic media that were or may have been used as a means to commit the offenses described on the warrant, including the receipt, possession, distribution, or transportation of child pornography in violation of Title 18, United States Code, Sections 2252(a)(4)(B) and 2252A(a)(2).

3. For any computer, computer hard drive, or other physical object upon which electronic data can be recorded (hereinafter, "COMPUTER") that is called for by this warrant, or that might contain things otherwise called for by this warrant:

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

- e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- f. evidence of the times the COMPUTER was used;
- g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- i. contextual information necessary to understand the evidence described in this attachment;
- j. evidence of the crimes described above in paragraph 1.

4. Records and things evidencing the use of the Internet, including:

- a. routers, modems, and network equipment used to connect computers to the Internet;
- b. records of Internet Protocol addresses used;
- c. records of Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

5. DEVICE UNLOCK: During the execution of the search of the property described in Attachment A, and with respect to (1) any device on John Boyden II’s person, or (2) any device at/on SUBJECT PREMISES reasonably believed to be owned, used, or accessed by John Boyden II, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of John Boyden II to the fingerprint scanner of the seized device(s); (2) hold the seized device(s) in front of the face of John Boyden II and activate

the facial recognition feature; and/or (3) hold the seized device(s) in front of the face of that John Boyden II and activate the iris recognition feature, for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this warrant.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

As used above, the term “COMPUTER” includes but is not limited to any and all computer equipment, including any electronic devices that are capable of collecting, analyzing, creating, displaying, converting, storing, concealing, or transmitting electronic, magnetic, optical, or similar computer impulses or data. These devices include but are not limited to any data-processing hardware (such as central processing units, memory typewriters, mobile “smart” telephones, tablets, and self-contained “laptop” or “notebook” computers); internal and peripheral storage devices (such as fixed disks, external hard disks, floppy disk drives and diskettes, thumb drives, flash drives, Micro SD cards, SD cards, CDs, DVDs, tape drives and tapes, optical storage devices, zip drives and zip disk media, and other memory storage devices); peripheral input/output devices (such as keyboards, printers, fax machines, digital cameras, scanners, plotters, video display monitors, and optical readers); and related communications devices (such as modems, routers, cables and connections, recording equipment, RAM or ROM units,

acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or
signaling devices, and electronic tone-generating devices); as well as any devices,
mechanisms, or parts that can be used to restrict access to such hardware (such as
physical keys and locks).